

In re Patent Application of:
KURDZIEL ET AL.
Serial No. **10/780,848**
Filing Date: **FEBRUARY 18, 2004**

REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application. The arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in independent Claim 1, for example, is directed to a cryptographic device comprising an input stage, and an intermediate stage connected to the input stage. The input stage receives an input data block and a key data block comprising a plurality of sub-key data blocks, and generates a plurality of first signals therefrom. The intermediate stage comprises a plurality of substitution units, each substituting data within a respective first signal. A diffuser is connected to the plurality of substitution units for mixing data to generate a diffused signal. An output stage is connected to the intermediate stage for repetitively looping back the diffused signal to the input stage for combination with a next sub-key data block.

Independent Claim 10 is directed to a communication system comprising a key scheduler, and a cryptographic device connected to the key scheduler, with the cryptographic device being similar to independent Claim 1.

Independent Claim 18 is directed to a method for converting an input data block into an output signal in a cryptographic device, and is similar to independent Claim 1.

In re Patent Application of:
KURDZIEL ET AL.
Serial No. **10/780,848**
Filing Date: **FEBRUARY 18, 2004**

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 10 and 18 over the Advanced Encryption Standard (AES) as disclosed by the Stein et al. published patent application. The Examiner has taken the position that Stein et al. discloses in FIG. 6 an input stage receiving an input data block and a key data block comprising a plurality of sub-key data blocks, and generating a plurality of first signals therefrom. The Examiner also characterized the intermediate stage as comprising substitution units **16** and a diffuser **18**, with the output stage corresponding to elements **24** and **26** as shown in FIG. 2.

The Applicants submit that the Examiner has mischaracterized Stein et al., particularly with respect to the substitution unit **16**. This unit **16** in Stein et al. does not correspond to the substitution unit as in the claimed invention.

Element **16** corresponds to an incoming data block that is to undergo an SBOX transformation by element **18**. Reference is directed to paragraph 32 of Stein et al., which provides:

"The AES algorithm subbyte transformation is effected using an S-BOX wherein the data block **16** is comprised of four words **30, 32, 34, 36** each of four bytes, S_{00} - S_{03} , S_{10} - S_{13} , S_{20} - S_{23} , and S_{30} - S_{33} ." (Emphasis added).

Still referring to FIG. 2, element **16** is applied as input to the SBOX transformation block **18**. There is no reference to element **16** receiving as input a key data block comprising a plurality of sub-key data blocks for generating a plurality of

In re Patent Application of:
KURDZIEL ET AL.
Serial No. **10/780,848**
Filing Date: **FEBRUARY 18, 2004**

first signals, as in the claimed invention. In FIG. 2 of Stein et al., the key data block **23** is downstream from the input stage providing the data block **16**. Similarly, in FIG. 6, the key data block **70** is a separate input from the input stage **12** receiving the input data block. Again, the key data block **70** is applied downstream from the input stage **12**.

Instead of element **16** corresponding to substitution units for substituting data within a respective first signal, element **16** corresponds to the data words **30, 32, 34, 36** that first undergo an SBOX transformation **18**, then a shift row transformation **20** followed by a mix column transformation **22** in which the key **23** is then added.

In sharp contrast, the claimed invention recites that the input stage receives an input data block and a key data block comprising a plurality of sub-key data blocks, and generates a plurality of first signals therefrom. The intermediate stage is connected to the input stage and comprises a plurality of substitution units, with each substituting data within a respective first signal. In Stein et al., the Examiner characterized element **16** as the substitution units when element **16** is actually the input data block; and Stein et al. also fails to disclose that element **16** receives as input the key data block - the key data block is instead added downstream from element **16**.

Accordingly, it is submitted that independent Claim 1 is patentable over Stein et al. Independent Claims 10 and 18 are similar to independent Claim 1. Therefore, it is submitted that these claims are also patentable over Stein et al.


In re Patent Application of:
KURDZIEL ET AL.
Serial No. **10/780,848**
Filing Date: **FEBRUARY 18, 2004**

In view of the patentability of independent Claims 1, 10 and 18, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330